Information Analysis and Infrastructure Protection

The Department of Homeland Security would merge under one roof the capability to identify and assess current and future threats to the homeland, map those threats against our current vulnerabilities, inform the President, issue timely warnings, and immediately take or effect appropriate preventive and protective action.

Threat Analysis and Warning. Actionable intelligence is essential for preventing acts of terrorism. The timely and thorough analysis and dissemination of information about terrorists and their activities will improve the government's ability to disrupt and prevent terrorist acts and to provide useful warning to the private sector and our population. Currently, the U.S. government has no institution primarily dedicated to analyzing systematically all information and intelligence on potential terrorist threats within the United States, such as the Central Intelligence Agency performs regarding terrorist threats abroad. The Department of Homeland Security, working together with enhanced capabilities in other agencies such as the Federal Bureau of Investigation would make America safer by pulling together information and intelligence from a variety of sources.

The prevention of terrorist acts requires a proactive approach that will enhance the capability of policymakers and law enforcement personnel to preempt terrorist plots and warn appropriate sectors. The Department would fuse and analyze legally accessible information from multiple available sources pertaining to terrorist threats to the homeland to provide early warning of potential attacks. This information includes foreign intelligence, law enforcement information, and publicly available information. The Department would be a full partner and consumer of all intelligence-generating agencies, such as the Central Intelligence Agency, the National Security Agency, and the FBI. By obtaining and analyzing this information, the Department would have the ability to view the dangers facing the homeland comprehensively, ensure that the President is briefed on relevant information, and take necessary protective action.

The Attorney General recently revised the guidelines governing how the FBI gathers information and conducts investigations. The new guidelines reflect the President's commitment to preventing terrorism by allowing the FBI to intervene and investigate promptly, while also protecting American's constitutional rights, when information suggests the possibility of terrorism. The revised guidelines empower FBI agents with new investigative authority at the early stage of preliminary inquiries, as well as the ability to search public sources for information on future terrorist threats. The FBI can now identify and track foreign terrorists by combining information obtained from lawful sources, such as foreign intelligence and commercial data services, with the information derived from FBI investigations. In addition, the revised guidelines removed a layer of "red tape" by allowing FBI field offices to approve and renew terrorism enterprise investigations rather than having to obtain approval from headquarters.

The Department of Homeland Security would complement the FBI's enhanced emphasis on counterterrorism law enforcement by ensuring that information from the FBI is analyzed side-by-side with all other intelligence. The Department and the Bureau would ensure cooperation by instituting standard operating procedures to ensure the free and secure flow of information and exchanging personnel as appropriate.

The Department's threat analysis and warning functions would support the President and, as he directs, other national decision-makers responsible for securing the homeland from terrorism. It would coordinate and, as appropriate, consolidate the federal government's lines of communication with state and local public safety agencies and with the private sector, creating a coherent and efficient system for conveying actionable intelligence and other threat information. The Department would administer the Homeland Security Advisory System and be responsible for public alerts.

The Department of Homeland Security would translate analysis into action in the shortest possible time – a critical factor in preventing or mitigating terrorist attacks, particularly those involving weapons of mass destruction. Because of the central importance of this mission, the Department would build excellence in its threat analysis and warning function, not only in terms of personnel, but also in terms of technological capabilities.

This proposal fully reflects the President's absolute commitment to safeguard our way of life, including the integrity of our democratic political system and the essential elements of our individual liberty. The Department of Homeland Security will not become a domestic intelligence agency.

Critical Infrastructure Protection. The attacks of September 11 highlighted the fact that terrorists are capable of causing enormous damage to our country by attacking our critical infrastructure – those assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale.

The Department of Homeland Security would coordinate a national effort to secure America's critical infrastructure. Protecting America's critical infrastructure is the shared responsibility of federal, state, and local government, in active partnership with the private sector, which owns approximately 85 percent of our nation's critical infrastructure. The new Department of Homeland Security will concentrate this partnership in a single government agency responsible for coordinating a comprehensive national plan for protecting our infrastructure. The Department will give state, local, and private entities one primary contact instead of many for coordinating protection activities with the federal government, including vulnerability assessments, strategic planning efforts, and exercises.

The Department would build and maintain a comprehensive assessment of our nation's infrastructure sectors: food, water, agriculture, health systems and emergency services, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), information and telecommunications, banking and finance, energy, transportation, chemical, defense industry, postal and shipping, and national monuments and icons. The Department would develop and harness the best modeling, simulation, and analytic tools to prioritize effort, taking as its foundation the National Infrastructure Simulation and Analysis Center (currently part of the Department of Energy). The Department would direct or coordinate action to protect significant vulnerabilities, particularly targets with catastrophic potential such as nuclear power plants, chemical facilities, pipelines, and ports, and would establish policy for standardized, tiered protective measures tailored to the target and rapidly adjusted to the threat.

Our nation's information and telecommunications systems are directly connected to many other critical infrastructure sectors, including banking and finance, energy, and transportation. The consequences of an attack on our cyber infrastructure can cascade across many sectors, causing widespread disruption of essential services, damaging our economy, and imperiling public safety. The speed, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. Accordingly, the Department of Homeland Security would place an especially high priority on protecting our cyber infrastructure from terrorist attack by unifying and focusing the key cyber security activities performed by the Critical Infrastructure Assurance Office (currently part of the Department of Commerce) and the National Infrastructure Protection Center (FBI). The Department would augment those capabilities with the response functions of the Federal Computer Incident Response Center (General Services Administration). Because our information and telecommunications sectors are increasingly interconnected, the Department would also assume the functions and assets of the National Communications System (Department of Defense), which coordinates emergency preparedness for the telecommunications sector.